

REMARKS

In this response, no claims are amended, no claims are canceled, and no claims are added; as a result, claims 1-15 are now pending in this application.

§102 Rejection of the Claims

Claims 1-15 were rejected under 35 U.S.C. § 102(e) for anticipation by Graunke et al. (U.S. 5,991,399). Applicant respectfully traverses the rejection of claims 1-15.

Claims 1-15 are not anticipated by, and are patentable, over Graunke et al. because Graunke et al. fails to disclose in a single prior art reference all of the elements included in each of claims 1-15,¹ as arranged in each of claims 1-15,² and so fails to show the identical claimed invention as included in claims 1-15.³ For example, claim 1 includes,

System for providing encrypted data to be used in a content player comprising a decryption device, comprising:

an encryption device for encrypting data using an encryption algorithm,

a protection device for providing secure device data, and for providing information on a protocol for communication between the content player and a secure device arranged to transform the secure device data into information required to decrypt the encrypted data, and

a control device for providing a protected contents structure containing the encrypted data, the secure device data, said protocol information and attribute data for finding relevant parts inside the protected contents structure,

wherein the attribute data comprises information to find in the protected contents structure information on **an appropriate protocol for establishing a communication interface between the content player and the secure device for use of the secure device to transform secure device data communicated to the secure device through the communication interface into information required to decrypt the encrypted data.** (Emphasis added).

¹ Anticipation requires the disclosure in a single prior art reference of each element of the claim under consideration. *W. L. Gore & Assocs. v. Garlock*, 721 F.2d 1540, 220 USPQ 303 (Fed. Cir. 1983), *cert. denied*, 469 U.S. 851 (1984).

² It is not enough, however, that the prior art reference discloses all the claimed elements in isolation. Rather, A[a]nticipation requires the presence in a single prior reference disclosure of each and every element of the claimed invention, *arranged as in the claim.*@ *Lindemann Maschinenfabrik GmbH v. American Hoist & Derrick Co.*, 730 F.2d 1452, 221 USPQ 481, 485 (Fed. Cir. 1984) (citing *Connell v. Sears, Roebuck & Co.*, 722 F.2d 1542, 220 USPQ 193 (Fed. Cir. 1983)) (emphasis added).

³ The identical invention must be shown in as complete detail as is contained in the ... claim.@ *Richardson v. Suzuki Motor Co.*, 868 F.2d 1226, 1236, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989); MPEP '2131.

Thus, claim 1 includes, "a protection device for providing secure device data, and for **providing information on a protocol for communication between the content player and a secure device** arranged to transform the secure device data into information required to decrypt the encrypted data." Further, claim 1 includes that, "attribute data comprises information to find in the protected contents structure information on **an appropriate protocol for establishing a communication interface between the content player and the secure device** for use of the secure device to transform secure device data communicated to the secure device through the communication interface into information required to decrypt the encrypted data." Applicant submits that at least this subject matter as included in claim 1 is not taught by Graunke et al., and so claim 1 is not anticipated by Graunke et al.

In contrast to claim 1, Graunke et al. states,⁴

An embodiment of the present invention includes a method of securely distributing a private key to a user's application program (also called a "trusted player" such as a digital versatile disk (DVD) player, compact disk read only memory (CD-ROM) player, or floppy disk device driver, and the like) with conditional access based on verification of the trusted player's integrity and authenticity. The trusted player can then use the private key to decrypt or sign a digital object. Conditional access to digital content is controlled because the trusted player is not pre-loaded with any key; each key is dynamically generated and communicated in real-time to the trusted player in a secure manner. Thus, the trusted player is not dependent on only one global key for decryption purposes of all digital content for the trusted player. Instead, each key is valid only for selected digital content (e.g., a particular movie, song, game, etc.). Additionally, the key is not nakedly transmitted to the trusted player, because the key could then be intercepted and copied. Instead, it is wrapped into a key module in which the key can only be used by the right trusted player as determined by the key module. The key module plugs in to the trusted player to validate the player and decrypt the content.

Thus, in contrast to claim 1, Graunke et al. concerns the distribution of a private key to a user's application program, also called a "trusted player" such as a DVD player, with conditional access on the basis of verification of the trusted player's integrity and authenticity. The private

⁴ See Graunke et al. at column 3, line 53 through column 4, line 7.

key in Graunke et al. is downloaded from a server to the trusted player in a secure manner. The key is wrapped into a key module in which the key can only be used by the right trusted player as determined by the key module.

However, there is no teaching in Graunke et al. of a secure device as included in the presently claimed subject matter, and so there is no teaching in Graunke et al. of "a protection device for providing secure device data, and for **providing information on a protocol for communication between the content player and a secure device** arranged to transform the secure device data into information required to decrypt the encrypted data," as required by claim 1.

The Office Action argues that the secure device of the presently claimed subject matter corresponds to the storage medium from Fig. 1 of Graunke et al. The cited portion of Graunke et al. referred to by the Office Action in support of this argument states,⁵

The removable storage medium may be a floppy disk, a CD-ROM, a DVD, or other data storage medium not yet developed. The storage medium includes digital content encrypted to provide protection against unauthorized use. The digital content may consist of any multimedia data, such as films, music, games, etc. The data on the storage medium is accessed by a program such as a storage device reader 16 via key module 18. The storage device reader forwards decrypted digital content to other application programs (not shown) for presentation or other use by a user (not shown). For example, the storage device reader may be a trusted DVD player and the digital content may be a feature film, the reader may be a CD-ROM player and the digital content may be a computer game, the reader may be a CD-ROM audio player and the digital content may be recorded music, etc. The storage device reader 16 interacts with a key module 18, which is downloaded from a communications network or otherwise accessed by the storage device reader. The key module 18 verifies that the storage device reader is authentic and that access to the digital content is allowed.

Thus, Graunke et al. describes the storage medium as a floppy disk, a CD-ROM, a DVD, or other data storage medium not yet developed, wherein the storage medium includes digital content encrypted to provide protection against unauthorized use. However, a description of a storage medium including digital content encrypted to provide protection against unauthorized

⁵ See Graunke et al. at column 4, lines 30-50.

use fails to teach "providing information on a **protocol for communication** between the content player and a secure device," as included in claim 1.

Further, since there is no teaching in Graunke et al. of providing information on a protocol for communication between the content player and a secure device, there is also no teaching in Graunke et al. of "attribute data comprises information to find in the protected contents structure information on **an appropriate protocol for establishing a communication interface between the content player and the secure device** for use of the secure device to transform secure device data communicated to the secure device through the communication interface into information required to decrypt the encrypted data," as also included in claim 1.

For at least the reasons stated above, Graunke et al. fails to teach all of the claimed subject matter included in claim 1, as arranged in claim 1. Therefore, claim 1 is not anticipated by Graunke et al.

In further examples of subject matter included in claims 1-15 and not taught by Graunke et al.:

Claim 3 includes,

System for decrypting encrypted data in a content player,
comprising:

an input for receiving protected contents containing encrypted data, secure device data, information on a protocol for communication between the content player and a secure device arranged to transform the secure device data into information required to decrypt the encrypted data, and attribute data for finding relevant parts inside the protected contents,

a decryption device, and

a control device,

wherein said secure device data comprises the information required to decrypt the encrypted data, and wherein the attribute data comprises information to find in the protected contents information on an appropriate protocol for communication between the content player and the secure device for retrieving the information required to decrypt the encrypted data, wherein the control device is programmed to use the attribute data to find the appropriate protocol information to establish a communication interface between the decryption device and a secure device used with the content player,

wherein the decryption device is suitable for communicating with the secure device as controlled by the

protocol information to obtain the information required by the decryption device to decrypt the encrypted data and generated by the secure device by transforming secure device data communicated to the secure device through the communication interface.

Claims 10 includes,

Method for providing a communication interface between a decryption device and a secure device in a content player, comprising:

- receiving a protected contents structure containing secure device data, information on a protocol for communication between the content player and a secure device arranged to transform the secure device data into information required to decrypt the encrypted data, and attribute data for finding relevant parts inside the protected contents structure, wherein said secure device data comprises the information required to decrypt the encrypted data, the attribute data comprising information to find in the protected contents structure information on an appropriate protocol for communication between the content player and the secure device for retrieving the information required to decrypt the encrypted data, and

- retrieving said protocol information from the protected contents structure to establish a communication interface between the decryption device and a secure device used with the contents player to transform secure device data communicated to the secure device through the communication interface into information required by the decryption device to decrypt encrypted data.

Claim 15 includes,

Method for broadcasting protected contents, comprising:

- encrypting data using an encryption algorithm,

- providing secure device data,

- providing information on a protocol for establishing a communication interface between a content player and a secure device arranged to transform the secure device data communicated to the secure device through the communication interface into the information required to decrypt the encrypted data,

- providing protected contents containing the encrypted data, the secure device data, the protocol information and attribute data, and

- broadcasting the protected contents,

wherein the attribute data comprises information to find in the protected contents information on an appropriate protocol for communication between the content player and the secure device.

For reasons analogous to those stated above with respect to claim 1, Graunke et al. fails to teach all of the claimed subject matter included in claim 3, and fails to teach all of the claimed subject matter included in claim 10, and fails to teach all of the claimed subject matter included in claim 15. Therefore, claims 3, 10, and 15 are not anticipated by Graunke et al.

Claim 2 depends from claim 1, claims 4-9 depend from claim 3, and claims 11-14 depend from claim 10. Thus, dependent claims 2, 4-9, and 11-14 include all of the claimed subject matter included in the independent claim from which they depend, and more. For at least the reasons stated above with respect to claims 1, 3, and 10, dependent claims 2, 4-9, and 11-14 are not anticipated by Graunke et al.

Because the Office Action fails to show how Graunke et al. teaches all of the claimed subject matter included in claims 1-15, the Office Action fails to meet its burden for establishing a *prima facie* case of anticipation with respect to claims 1-15. Applicant respectfully requests withdrawal of the 35 U.S.C. § 102 rejection, and allowance of claims 1-15.

Reservation of Rights

Applicant does not admit that references cited under 35 U.S.C. §§ 102(a), 102(e), 103/102(a), or 103/102(e) are prior art, and reserves the right to swear behind them at a later date. Arguments presented to distinguish such references should not be construed as admissions that the references are prior art.

CONCLUSION

Applicant respectfully submits that the claims are in condition for allowance, and notification to that effect is earnestly requested. The Examiner is invited to telephone Applicant's attorney at 612-371-2132 to facilitate prosecution of this application.

If necessary, please charge any additional fees or credit overpayment to Deposit Account No. 19-0743.

Respectfully submitted,

WILHELMUS GERARDUS PETRUS MOOIJ

By his Representatives,

SCHWEGMAN, LUNDBERG, WOESSNER & KLUTH, P.A.
P.O. Box 2938
Minneapolis, MN 55402
408-278-4042

Date DECEMBER 19/2006

By Robert B. Madden

Robert B. Madden
Reg. No. 57,521

CERTIFICATE UNDER 37 CFR 1.8: The undersigned hereby certifies that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail, in an envelope addressed to: Mail Stop Amendment, Commissioner of Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on this 19 day of December 2006.

Dawn R. Shaw
Name

Dawn R. Shaw
Signature